The Honorable Richard A. Jones

UNITED STATES DISTRICT COURT FOR THE
WESTERN DISTRICT OF WASHINGTON
AT SEATTLE

UNITED STATES OF AMERICA, Plaintiff v. ROMAN V. SELEZNEV, Defendant.	NO. CR11-0070RAJ **TRIAL BRIEF** **TRIAL DATE: August 15, 2016**

I. INTRODUCTION

Defendant Roman Seleznev is charged in a 40-count Second Superseding Indictment with various crimes arising out of an international computer hacking and credit card fraud scheme that Seleznev orchestrated between 2007 and 2014. Specifically, Seleznev hacked into the computer systems of hundreds of businesses (many of them pizza restaurants) in the Western District of Washington and around the world. Seleznev installed malicious software on his victims' computer systems that allowed him to steal the credit card data of their customers. Seleznev, using the nicknames "nCuX," "Track2," "Bulba," and "2Pac," then sold the stolen credit card data on automated websites. Seleznev's customers used the data to make fraudulent credit card purchases, resulting in a current known fraud loss of approximately $170 million.

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5200
SEATTLE, WASHINGTON 98101
(206) 553-7970

Trial is scheduled for August 15, 2016. The government expects to call approximately 20 witnesses. The government anticipates that it will complete the presentation of its case-in-chief in 12 trial days. AUSA Seth Wilkinson will deliver the opening statement. With the Court's permission, the government will split closing arguments, with AUSA Norman Barbosa delivering the closing argument and Department of Justice Trial Attorney Harold Chun delivering the rebuttal. Mr. Chun will also represent the United States during *voir dire.*

II. BACKGROUND AND SUMMARY OF EVIDENCE

A. Overview

The charges stem from Seleznev's participation in the international online "carding" community. "Carding" is a term used to describe criminal computer hacking for the purpose of stealing and trafficking in credit card data. "Carders" advertise stolen credit card data, share information, and trade hacking tools and other related goods and services anonymously on underground internet forums known as "carding forums." Carding forum participants use alias nicknames known as "nics," which allow them to maintain anonymity while building an online reputation.

The Second Superseding Indictment alleges that, between 2007 and 2014, Seleznev hacked into businesses' credit card processing systems known as point of sale ("POS") systems, where he would install malware designed to collect credit card numbers processed by the businesses. The malware would then periodically send the credit card numbers to computer servers controlled by Seleznev. Seleznev offered the stolen credit card numbers for sale over the internet with the intent that the purchaser would use the numbers for fraudulent transactions.

Defendant used various nics over the course of his criminal career. Between 2002 and 2009, Seleznev operated under the nic "nCuX," which is the transliteration of the Russian word for "psycho." Between 2009 and 2012, Seleznev used the nic "Track2," and operated automated vending sites with the names "Track2" and "Bulba." Finally,

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5200
SEATTLE, WASHINGTON 98101
(206) 553-7970

between February 2013 and his capture on July 5, 2014, defendant used the nic "2Pac" and operated websites with the names "2Pac" and "POS Dumps."

B. Defendant's Criminal Identities

1. nCuX

The evidence will show that an individual using the online nic nCuX began participating in the international carding community in approximately 2002. The United States Secret Service ("Secret Service") began monitoring nCuX's activity in 2005. Through the review of underground carding forums, the Secret Service learned that nCuX was active on several carding forums including Carder.org, and CarderPlanet.

Carding forum records show that in approximately 2007, nCuX began selling stolen credit card data over the internet. Between 2007 and 2009, nCuX regularly offered for sale large volumes of stolen credit cards by placing advertisements on the carding forums for "bases," a slang term for batches of stolen credit card data, to customers who would later use the stolen data to commit credit card fraud.

As a result of nCuX's active online presence, the Secret Service identified nCuX as a top-tier target. On May 19, 2009, Secret Service agents met with Russian law enforcement authorities and disclosed to the Russian authorities their knowledge of nCuX's activities, as well as their suspicions that nCuX was a Russian national named Roman Seleznev. Just one month later, on June 21, 2009, nCuX posted an announcement stating that he was going out of business. nCuX then completely disappeared from the Internet.

2. Track2 and Bulba

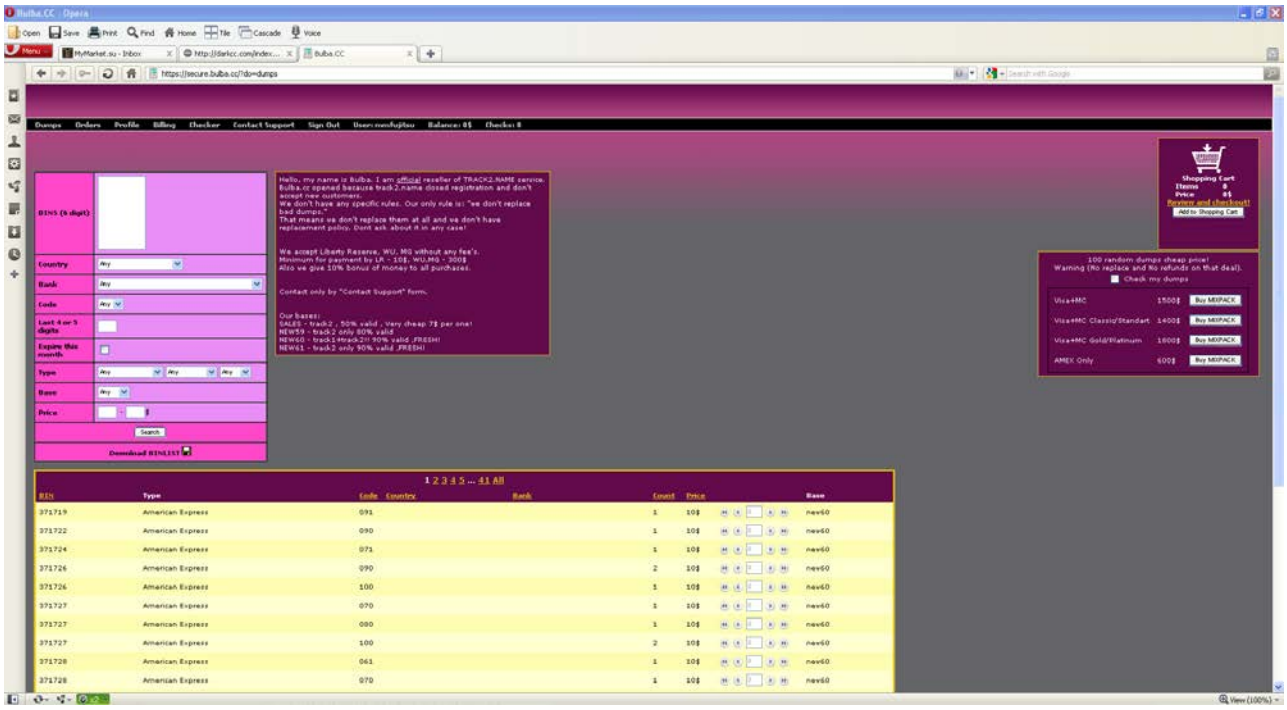
Following nCuX's disappearance from the internet, a new carder using the nic "Track2" appeared on the same carding forums previously frequented by nCuX. On September 26, 2009, Track2 appeared on the carding forum Carder.su and announced the opening of an automated vending site with the web address "track2.tv."

Automated vending sites like the Track2 site are websites that facilitate the automatic mass sale of stolen credit card data. While these sites are devoted to credit

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5200
SEATTLE, WASHINGTON 98101
(206) 553-7970

card fraud, their design and operation is similar to legitimate online retailers such as Amazon. Customers search for stolen credit card numbers meeting certain specifications. For example, customers may search for credit cards issued by a particular bank. Once the customer has identified the numbers he or she wishes to purchase, he or she places items in a shopping cart and purchases the stolen information using difficult-to-trace e-currency payment methods such as Liberty Reserve, Web Money, or Bitcoin.

In April 2010, while the Track2 site was still operating, Track2 began directing existing and potential customers to another site with the address "bulba.cc." Track2's online posts described bulba.cc as "our official reseller." Bulba was almost identical to the Track2 sites in appearance and function. Below is a screenshot of the bulba website:



Seleznev was seriously injured in Morocco in April 2011. Following the accident, undercover law enforcement visits to the bulba website found the website was failing to update its stolen credit card data. On December 30, 2011, Track2 posted an announcement that he was closing his sites as of January 7, 2012 because "[we] don't have more dumps." Track2 and Bulba subsequently disappeared from the internet.

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5200
SEATTLE, WASHINGTON 98101
(206) 553-7970

3. 2Pac and POS Dumps

In February 2013, a carder using the nic "2pac" appeared on the internet. 2pac established a presence on carding forums and began selling credit card numbers on an automated vending site at the domain "2pac.cc." 2pac promoted his site as "the Best Dumps Market."

The 2pac website resembled the bulba and Track2 websites in appearance. However, unlike those two sites, the 2pac site not only sold card data that the website operator had himself compromised; it also served as a reseller, purchasing blocks of stolen card data from other hackers and selling that data on consignment. In 2013, and in the first half of 2014, 2pac.cc was one of the major vendors of stolen credit cards on the internet. 2Pac offered for sale card data traced to numerous major retail point-of-sale breaches including Target, Neiman Marcus, Michaels, Staples and Home Depot.

2Pac also operated a second website known as "POS Dumps." POS Dumps served the dual purposes of training potential customers on how to use stolen credit card data, and channeling the potential customers to the 2Pac website. The front page of this website contained the following introduction:

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5200
SEATTLE, WASHINGTON 98101
(206) 553-7970

POSDumps.com instructed users on how to purchase stolen credit card data, and how to re-encode the data onto blank credit cards for use in fraudulent purchases. The POSDumps.com website contained advertisements for 2pac.cc and commentary encouraging users to purchase their dumps at 2pac.cc.

C. The Secret Service Investigation

In the summer of 2010, Seattle Police Detective David Dunn, a member of the Seattle Secret Service Electronic Crimes Task Force, was asked to investigate an intrusion into the POS systems at a Schlotzky's Deli in Coeur d'Alene, Idaho. Detective Dunn's investigation led him to the bulba.cc and track2.name vending sites, where data stolen during the Schlotzky's intrusion had been sold. Then, Detective Dunn was asked to respond to a number of intrusions at businesses in the Western District of Washington, including Seattle businesses such as Broadway Grill, Mad Pizza and Grand Central Baking. In investigating these hacks, Detective Dunn found that the malicious software installed on these victims was similar to that installed at Schlotzky's.

By analyzing the victim computers, Detective Dunn was able to determine the methods of intrusion and map out parts of Track2's computer infrastructure. Detective Dunn found that the intruder had scanned the internet for open "ports"—pathways intended to allow an offsite IT specialist to remote access a business's computer system to perform maintenance. After identifying a system with an open port, the intruder obtained remote access to the computer and installed malware (malicious software) on victims' machines. The malware searched the computer systems for credit card data, which it would then collect and periodically send to servers known as "collection servers" controlled by the intruder. The intruder would then offer the stolen data for sale on the Track2 and Bulba websites.

Detective Dunn partnered with Special Agent Keith Wojcieszek, a Washington DC-based Secret Service agent who was also investigating Track2. Both Detective Dunn and Special Agent Wojcieszek conducted undercover operations in which they visited the Track2 and Bulba websites. Detective Dunn and Special Agent Wojcieszek both

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5200
SEATTLE, WASHINGTON 98101
(206) 553-7970

established undercover accounts on the Bulba site and purchased stolen credit cards from the site.

Detective Dunn and Special Agent Wojcieszek identified the infrastructure (servers and email accounts) that Track 2 used to operate his business. In cases where the infrastructure was located in the United States, they obtained search warrants to look for evidence of Track2's true identity. As discussed below, this investigation developed overwhelming evidence that Roman Seleznev is nCuX, Bulba and Track2.

D. Evidence Identifying Roman Seleznev as Track2, Bulba and nCuX

1. The HopOne Server

Among the servers used to collect Track2's stolen credit cards was a server known as the "HopOne" server. Unlike other collection servers used by Track2, the HopOne server was located in the United States (in Virginia) and was therefore subject to U.S. process. On January 19, 2011, Special Agent Wojcieszek obtained a search warrant in the Eastern District of Virginia to search the HopOne server and two related servers at the same location. A search of the HopOne server revealed that the server had been used to collect hundreds of thousands of credit card numbers stolen from compromised retailers around the world, including the ones in the Western District of Washington that Detective Dunn had been investigating.

The search of the HopOne server also revealed numerous forensic artifacts linking the server to Roman Seleznev. For example, a forensic analysis found remnants of web browsing history showing that the user of the HopOne server had made multiple travel reservations for Roman Seleznev using that server. The reservations contained Seleznev's date of birth and passport number, along with the names of his wife, daughter, nanny, mother and father in law, and two known associates. Analysis of the HopOne server also showed that the user had used two email accounts: Romariogro@mail.ru (which was found on defendant's laptop and iPhone at the time of his arrest) and rubensamvelich@yahoo.com (which has numerous links to Seleznev discussed below).

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5200
SEATTLE, WASHINGTON 98101
(206) 553-7970

2. Boookscafe@yahoo.com

Track2 used several Yahoo! email accounts to operate his enterprise. One of these was an account with the address "boookscafe@yahoo.com" (the "Boookscafe Account"). The Boookscafe Account was used to register several nCuX-related domains in 2009.[1] The Boookscafe Account was also used to manage the server known as the "smaus" or "shmak" server, which hosted the malware Track2 installed on victim machines.

Special Agent Wojcieszek obtained a warrant to search the Boookscafe Account. The search produced extensive e-mail evidence confirming that nCuX and Track2 had used the Boookscafe Account to manage the nCuX and Track2 carding operations. For example, the account received billing statements for the "smaus" server (Track2's malware repository) and emails confirming registration of nCuX websites. It also included numerous emails addressed to nCuX discussing the purchase and sale of stolen credit card data.

The Boookscafe Account also contained overwhelming evidence showing that Roman Seleznev was the user of the account. The evidence includes the following:

- Emails to Seleznev from Seleznev's wife, Svetlana Selezneva, attaching pictures of herself and their daughter;
- E-mails addressed to "Roman Seleznev" from the Russian social media site Vkontakte;
- Invoices from a Russian online flower business, sendflowers.ru, addressed to Roman Seleznev with details of flower orders placed by Mr. Seleznev to be delivered to Svetlana Selezneva at Roman Seleznev's home address; and
- An invoice addressed to Seleznev from the Russian online retailer "Internet Store – Defencer" for the purchase of an external microphone in September 2009 listing a phone number known to be used by Seleznev.

In addition, the Boookscafe Account also contained several e-mails showing that the user frequently opened internet accounts with the user name "smaus" and the

[1] To open a website, a person is required to provide certain registration information, including his name and email address to a domain name registrar. While criminals often use fictitious names to register criminal websites, they must use a valid email account so that they can respond to any issue raised by the registrar.

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5200
SEATTLE, WASHINGTON 98101
(206) 553-7970

password "ochko." For example, the user opened an investment account using "smaus1" and "ochko123" as the username and password, respectively. A forensic examination of the laptop seized from Seleznev during his arrest later revealed that Seleznev's user account for his laptop was named "smaus" and the password was "ochko123." Seleznev's laptop also contained several password "cheat sheets" (lists of passwords and usernames). The "cheat sheets" showed that Seleznev frequently used "smaus" and "ochko" as usernames and passwords.

3. Rubensamvelich@yahoo.com

The investigation found that Track2 also used a second Yahoo account with the address rubensamvelich@yahoo.com (the "Rubensamvelich Account") to operate his enterprise. For example, Track2 used the Rubensamvelich Account to register the Track2 automated vending sites. Track2 also used this email account to manage the HopOne server discussed above.

Detective Dunn and Special Agent Wojcieszek obtained a search warrant for the Rubensamvelich Account. Again, the search confirmed that Track2 had used the account for his criminal activity. For example, the account contained emails pertaining to the registration of the Track2 sites, emails discussing the purchase and sale of credit card data, and emails in which Track2 contracted with computer service providers to provide services for the Track2 site.

As with the Boookscafe Account, the search of the Rubensamvelich Account revealed links to Roman Seleznev. For example, the account included an e-mail from PayPal dated September 19, 2009, addressed to "Roman Seleznev," and listing Seleznev's known Vladivostok address. The account contained a receipt for the purchase of a travel guide to Bali purchased during a period when defendant was in Indonesia. The account also contained dozens of e-mails showing that the user of the account frequently used the words "smaus" and "ochko123" as his password and login information.

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5200
SEATTLE, WASHINGTON 98101
(206) 553-7970

4. bulbacc@yahoo.com

Track2 used an email account with the address bulbacc@yahoo.com (the "Bulba Account") to register the "bulba" automated vending site. Detective Dunn and Special Agent Wojcieszek also obtained a warrant to search this account. The search showed that the Bulba Account received very little use and did not itself contain evidence explicitly linking the account to Seleznev. However, the account did contain records showing that the login and password for the email account were "bulbacc" and "telkom135," respectively. Agents later found this login and password account information saved on the password "cheat sheet" that Seleznev maintained on his personal laptop.

5. Liberty Reserve Data

Track2 collected payments for the credit card data he sold using a Costa Rica-based digital currency service known as Liberty Reserve. Liberty Reserve allowed users to remain anonymous, and for this reason was widely used as a payment system for criminal transactions. The Secret Service seized Liberty Reserve's servers in May 2013 in connection with a federal indictment against the operators of the site.[2]

At trial, the government will offer account records seized from Liberty Reserve that establish links between Seleznev and his online nics. Specifically, registration data from numerous Liberty Reserve accounts will show that the accounts were opened with information connected to Seleznev, such as his true name, date of birth, and home address in Vladivostok, Russia. The Liberty Reserve accounts were also opened with email accounts linked to Seleznev such as the Rubensamvelich Account and romariogrol@mail.ru. Additionally, connection logs for defendant's numerous accounts will show that the accounts were accessed by similar IP addresses, thereby connecting them together. Furthermore, transaction records will show that transactions were noted with comments referring to defendant's true name, bulba.cc, track2 and "dumps." The

[2] In January 2016, the founder of Liberty Reserve plead guilty to conspiring to commit money laundering. In May 2016, he was sentenced to 20 years prison. See https://www.justice.gov/opa/pr/liberty-reserve-founder-sentenced-20-years-laundering-hundreds-millions-dollars.

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5200
SEATTLE, WASHINGTON 98101
(206) 553-7970

transaction records will also indicate that within approximately four years, defendant's accounts received more than 17 million dollars in deposits from more than 67,000 transactions. Lastly, agents will testify that they later found login information for some of the Liberty Reserve accounts on the password "cheat sheet" that Seleznev maintained on his personal laptop.

E. Evidence Seized During Defendant's Arrest

1. Charges and Arrest

On March 16, 2011, a grand jury in this district charged Seleznev with 29 felony counts arising out of his computer intrusions into businesses in the Western District of Washington. Defendant remained at large until July 5, 2014, when he was apprehended in Male, the capital of the island nation of the Maldives, with the assistance of Maldivian authorities. At the time of his arrest, Seleznev was carrying a laptop computer, an iPhone, his passport, and other pieces of evidence, all of which were seized by the arresting agents.

Defendant has repeatedly challenged the circumstances of his arrest, arguing that he was "kidnapped" in violation of international law. This claim was rejected first by the district Court in Guam (where defendant was taken immediately after his arrest) and then by this Court. Despite these rulings, defense counsel has continued to state in open court that his client was kidnapped. The government has separately moved *in limine* to prohibit counsel from making these improper statements in the presence of the jury. Dkt 359.

2. The Laptop

On July 28, 2014, the Honorable James P. Donohue authorized a warrant for the search of defendant's laptop and iPhone. Secret Service agents discovered overwhelming evidence on the laptop demonstrating that Seleznev was the true identity of nCuX, Track2, Bulba, and 2Pac. The evidence on the laptop includes, but is not limited to:

- Approximately 250 "dump files" containing card data for approximately 1.7 million stolen credit cards;

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5200
SEATTLE, WASHINGTON 98101
(206) 553-7970

- An electronic password "cheat sheet" that contained the logon IDs and passwords for carding-related accounts, including the bulba and 2Pac sites. The most frequently-used logon ID and password were "ochko" and "smaus"—the same credentials used by Track2 on the Boookscafe Account and Rubensamvelich Account;
- The pictures, text, and other raw file materials used to create the "POS Dumps" website;
- Evidence that the user of the laptop repeatedly logged onto various websites, including the 2Pac website, using the name "2Pac;
- Chats between 2Pac and other carders discussing the purchase and sale of stolen credit card data; and
- Evidence that, just two days before his apprehension, Seleznev had logged on to the U.S. Courts' Pacer website and conducted criminal case searches on the Pacer system for the names "Seleznev," "Bulba," and "2pac."

On May 10, 2016, Seleznev moved to suppress all evidence obtained from the laptop, arguing that the laptop had been mishandled by Secret Service forensic analysts, and that post-seizure file activity indicated that the computer had been subject to tampering. On June 23, 2016, the Court denied the motion, finding that the "overwhelming weight of the evidence" indicates that the post-seizure activity was the result of normal background and operating system activity, and was not caused by a user.

3. The iPhone

The search of Seleznev's iPhone produced additional evidence of Seleznev's criminal activity. For example, the government will present the following evidence retrieved from Seleznev's iPhone:

- Emails reflecting Seleznev's use of the "smaus" and "ochko" login and password;
- Emails reflecting Seleznev's use of the "Romariogro" email account; the same email used by the user of the HopOne server and relevant Liberty Reserve accounts;
- A photograph of a chat between 2Pac and another carder; and
- Evidence of unexplained wealth, including photographs of packages of large amounts of cash, and defendant with high-end automobiles.

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5200
SEATTLE, WASHINGTON 98101
(206) 553-7970

F. Evidence of Post-Arrest Activity

Following Seleznev's arrest, the 2pac.cc vending site experienced a downturn similar to what was seen on the bulba.cc vending site following defendant's injury in April 2011. Customers began complaining that updates were infrequent and that the proprietor of the shop had gone silent and was no longer responding to customer support inquires. A few weeks after defendant's arrest, someone posted a message apologizing for the extended outage and stated that new cards would soon be added to the inventory. The message, which was dated August 8, 2014, explained that the proprietor of the shop was unreachable because he was hospitalized following a "car accident."

The site continued to operate until August 15, 2014. On that day, at Seleznev's detention hearing, the government revealed that it believed Seleznev was the true identity behind 2pac. The site went dead within hours of the hearing. The site briefly went back online in September 2014, but the following month was seized by the German Federal Police at the request of the United States Department of Justice.

III. CHARGES AND RELEVANT LAW

A. Procedural Background

As noted above, the grand jury originally charged Seleznev in a 29-count indictment on March 3, 2011. The original indictment charged Seleznev with his criminal activities under the nics "nCuX," "Track2," and "Bulba." That indictment was superseded on March 16, 2011 to make a minor technical change.

In early 2014, the USSS began developing evidence that Seleznev was the true identity of "2Pac." On October 8, 2014, following Seleznev's arrest, the grand jury charged Seleznev in a 40-count Second Superseding Indictment that adds charges for Seleznev's conduct using the "2pac" nic, including a 2013 intrusion into Red Pepper Pizza in Duvall, Washington.

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5200
SEATTLE, WASHINGTON 98101
(206) 553-7970

This matter was originally set for trial on October 6, 2014. Seleznev subsequently substituted attorneys four times and requested and received four continuances of the trial date. Trial is now scheduled for August 15, 2016.

B. Charges

1. Counts 1-11: Wire Fraud

The Charges and Elements: Counts 1 through 11 charge Seleznev with wire fraud in violation of 18 U.S.C. § 1343. The charges allege that the defendant participated in a scheme to defraud banks and merchants through the fraudulent presentation of stolen credit card data. There are two types of charged wire transmissions: (a) incidents in which Seleznev caused the transmission of malware onto victim computers in this district (counts 1-8 and 11); and (b) incidents in which Seleznev caused the transmission of stolen credit card data from victim machines in this district to collection servers located outside of Washington (counts 9 and 10).

The Ninth Circuit model wire fraud instruction sets out the following elements:

> First, the defendant knowingly participated in a scheme or plan to defraud, or a scheme or plan for obtaining money or property by means of false or fraudulent pretenses, representations, or promises;
>
> Second, the statements made or facts omitted as part of the scheme were material; that is, they had a natural tendency to influence, or were capable of influencing, a person to part with money or property;
>
> Third, the defendant acted with the intent to defraud; that is, the intent to deceive or cheat; and
>
> Fourth, the defendant used, or caused to be used, a wire communication to carry out or attempt to carry out an essential part of the scheme to defraud.

Ninth Circuit Model Instruction 8.124. The government need not prove justifiable reliance or damages; nor need it show that the scheme was successful. *Id.*; see *Neder v. United States*, 527 U.S. 1, 25 (1999).

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5200
SEATTLE, WASHINGTON 98101
(206) 553-7970

The government has proposed this model instruction, but has suggested that the fourth element be modified to make clear that the wiring must be an interstate or international wire transmission. *United States v. Jinian*, 725 F.3d 964, 965 (9th Cir. 2013) (wire must be interstate, though defendant need not be aware of its interstate nature). Following is a discussion of principles relevant to certain elements of this offense:

Scheme to Defraud: A scheme to defraud may be proven by evidence that the defendant sought to obtain money or property by false representations, deceitful statements, half-truths, or the concealment of material facts. *United States v. Beecroft*, 608 F.2d 753, 757 (9th Cir. 1979) (mail fraud statute); *United States v. Allen*, 554 F.2d 398, 410 (10th Cir. 1977). The government need not prove a specific false statement was made. *See Ninth Circuit Model Jury Instructions* 8.123 (2010 Edition) (*quoting United States v. Woods*, 335 F.3d 993, 999 (9th Cir. 2003) ("Rather there are alternative routes to a . . . conviction, one being proof of a scheme or artifice to defraud, which may or may not involve any specific false statements."). "[T]he words 'to defraud' have the common understanding of wronging one in his property rights by dishonest methods or schemes and usually signify the deprivation of something of value by trick, deceit, chicane or overreaching." *Carpenter v. United States*, 484 U.S. 19, 27 (1987) (citations omitted).

Use of the Wires: The United States must prove that the defendant caused an interstate or foreign wire communication to be used in furtherance of the scheme. The law does not require that the defendant personally cause the wire transmission. *United States v. Jones*, 712 F.2d 1316, 1320 (9th Cir. 1983). Rather, it is enough that the defendant knows that a wire will be used in the ordinary course of business or can reasonably foresee such use. *Id.*; *United States v. Lothian*, 976 F.2d 1257, 1262 63 (9th Cir. 1992). Furthermore, the wire communication need not itself contain a false representation to be in furtherance of a scheme to defraud. The government need only show that the communication was "incident to an essential part of the scheme. *Schmuck v. United States*, 489 U.S. 705, 711 (1989). Each separate wire communication in

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5200
SEATTLE, WASHINGTON 98101
(206) 553-7970

furtherance of the scheme to defraud constitutes a separate violation of the wire fraud statute. *United States v. Vaughn*, 797 F.2d 1485, 1493 (9th Cir. 1986). Here, the charged wirings were in furtherance of the scheme to defraud because they were the means by which Seleznev stole the credit card data that was ultimately presented to merchants in the fraudulent transactions.

Co-Schemer Liability: "[W]ire fraud [is] treated like conspiracy in several respects." *United States v. Stapleton*, 293 F.3d 1111, 1117 (9th Cir. 2002). "[A]cts of co-participants in a scheme to defraud are admissible against other participants, just as in a conspiracy charge." *Id.;* see *Lothian*, 976 F.2d at 1263 ("[l]ike co-conspirators, knowing participants in the scheme are legally liable for their co-schemers' use of the mails or wires"). Therefore, the government does not need to show that defendant personally committed each element of the offense. Rather, it is sufficient to show that each element was committed either by defendant or by a co-participant in the scheme to defraud.

Verdict Form Provision Regarding "Affects a Financial Institution": The grand jury alleged in the Second Superseding Indictment that defendant's acts of wire fraud "affected a financial institution." A defendant's acts of wire fraud "affect a financial institution" if those acts cause a new or increased risk of loss to the financial institution. *United States v. Stargell*, 738 F.3d 1018, 1022 (9th Cir. 2013).

Affecting a financial institution is not a necessary element of liability under Section 1343. However, if the petite jury concludes that the wire fraud did indeed affect a financial institution, this would increase the statutory maximum from 20 years to 30 years. 18 U.S.C. § 1343. Accordingly, the government is proposing a verdict form that allows the jury to make this specific finding. The proposed verdict forms first asks the jury for a finding on whether the four elements of the offense are satisfied, *i.e.*, whether Seleznev is guilty of wire fraud. If the jury reaches a guilty verdict on any count of wire fraud, the verdict form asks the jury to determine whether the crime affected a financial institution.

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5200
SEATTLE, WASHINGTON 98101
(206) 553-7970

2. Counts 12-20: Intentional Damage to a Protected Computer

The Charges and Elements: Counts 12-20 charge Seleznev with intentional damage to a protected computer in violation of 18 U.S.C.§ 1030(a)(5)(A). This statute makes it a crime to "knowingly cause[] the transmission of a program, information, code, or command, and as a result of such conduct, intentionally cause[] damage without authorization, to a protected computer." The statute defines "protected computer" to include any computer "used in or affecting interstate commerce." 18 U.S.C. § 1030(e)(2)(B).

These charges allege that Seleznev damaged the specified victim computers by installing malicious software on those computers. The government has proposed the Ninth Circuit model instruction, which sets forth the following elements:

> First, the defendant knowingly caused the transmission of a program, information, code, or command to a computer;
>
> Second, as a result of the transmission, the defendant intentionally impaired, without authorization, the integrity of a program or system; and
>
> Third, the computer was used in or affected interstate or foreign commerce or communication.

Ninth Circuit Model Jury Instruction 8.100. A discussion of certain relevant legal issues follows.

Damage: Section 1030 defines "damage" to include "any impairment to the integrity of data." 18 U.S.C. § 1030(e)(8). Courts have held that the implantation of malware and similar conduct constitutes "damage" under Section 1030(a)(5)(A). *United States v. Makwana*, 445 F. Appx. 671, 673 (4th Cir. 2011) (affirming §1030(a)(5)(A) conviction and resulting application of USSG enhancement where defendant inserted malicious code onto server, even though malicious code was discovered prior to its execution); see also *United States v. Middleton*, 231 F.3d 1207, 1208-1209, 1212-1213 (9th Cir. 2000) (affirming §1030(a)(5)(A) conviction where defendant's unauthorized access "allowed Defendant to take advantage of the benefits

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5200
SEATTLE, WASHINGTON 98101
(206) 553-7970

and privileges associated with that employee's account, such as creating and deleting accounts and adding features to existing accounts."); *Shurgard Storage Centers, Inc. v. Safeguard Self Storage, Inc.*, 119 F. Supp. 2d 1121, 1126-27 (W.D. Wash. 2000) (denying motion to dismiss civil 1030(a)(5)(C) charge where "no data was physically changed or erased, but . . . an impairment of its integrity occurred").

Verdict Form Provision Regarding Loss: A violation of Section 1030(a)(5)(C) is punishable by up to ten years of imprisonment if the offense caused loss of loss of at least $5,000 in any one-year period; otherwise the crime is punishable as a misdemeanor. 18 U.S.C. § 1030(a)(4)(B)(1). The government's proposed verdict form asks the jury to determine whether this condition is satisfied.

3. Counts 21-29: Obtaining Information From a Protected Computer

The Charges and Elements: Counts 21-29 charge Seleznev with obtaining information from a protected computer in violation of 18 U.S.C.§ 1030(a)(2). Section 1030(a)(2) makes it a crime to "intentionally access a computer without authorization" and thereby obtain "information from any protected computer." As discussed above, any computer used in interstate or foreign commerce is a "protected computer." Here, the indictment alleges that Seleznev violated the statute in nine instances by hacking into victim computers, installing malware, and obtaining credit card numbers from the victim machines.

The government has proposed the Ninth Circuit model instruction for this offense, which sets forth the following elements:

> First, the defendant intentionally accessed without authorization a computer; and
>
> Second, by accessing without authorization a computer, the defendant obtained information from a computer that was used in or affected commerce or communication between one state and other states, or between a state of the United States and a foreign country.

Ninth Circuit Model Jury Instruction 8.97. The Ninth Circuit has held that a person accesses a computer "without authorization" under this statute when a "hacker accesses

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5200
SEATTLE, WASHINGTON 98101
(206) 553-7970

someone's computer without permission." *LVRC Holdings LLC v. Brekka*, 581 F.3d 1127, 1135 (9th Cir. 2009); *see United States v. Nosal*, -- F.3d --, 2016 WL 3608753, *8-9 (9th Cir. July 5, 2016) (reaffirming *Brekka's* definition of "without authorization").

Verdict Form Provision Regarding Financial Gain and other Criminal Acts: A violation of Section 1030(a)(2) is punishable by up to five years of imprisonment if the offense was committed for commercial advantage or private financial gain, or if the offense was committed in furtherance of any criminal or tortious act. 18 U.S.C.§ 1030((c)(2)(B)(i) and (ii)**.** Otherwise, the offense is punishable as a misdemeanor. The government's proposed verdict form asks the jury to determine whether this condition is satisfied.

4. Counts 30-38: Possession of 15 or More Unauthorized Access Devices

The Charges and Elements: Counts 30-38 charge Seleznev with possession of 15 or more unauthorized access devices in violation of 18 U.S.C.§ 1029(a)(3). This statute makes it a crime to "knowingly and with intent to defraud posses[s] fifteen or more . . . unauthorized access devices." The indictment charges defendant with nine incidents of possessing 15 or more access devices by collecting credit card data stored on victim computers. The Ninth Circuit Model Instruction sets out the following elements:

> First, the defendant knowingly possessed at least fifteen unauthorized access devices at the same time;
>
> Second, the defendant knew that the devices were unauthorized;
>
> Third, the defendant acted with the intent to defraud; and
>
> Fourth, the defendant's conduct in some way affected commerce between one state and other states, or between a state of the United States and a foreign country.

Access Device: The term "access device" means:

> any card, plate, code, account number, electronic serial number, mobile identification number, personal identification number . . . or other means of account access that can be used, alone or in conjunction with

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5200
SEATTLE, WASHINGTON 98101
(206) 553-7970

> another access device, to obtain money, goods, services, or any other thing of value, or that can be used to initiate a transfer of funds.

18 U.S.C. § 1029(e)(1); *see* Ninth Circuit Model Instruction 8.90. A credit card number is an access device. *United States v. Onyesoh*, 674 F.3d 1157, 1169 (9th Cir. 2012).

Possession: "A person has possession of something if the person knows of its presence and has physical control of it, or knows of its presence and has the power and intention to control it." *United States v. Cain*, 130 F.3d 381, 382 (9th Cir. 1997). The government has proposed Ninth Circuit Model Instruction 3.17, which provides this definition. Defendant "possessed" the credit card data at issue under this definition because he collected it on the victims' computer systems and exerted control over the data by sending it to his collection servers.

5. Counts 39-40: Aggravated Identity Theft

Counts 39 and 40 charge Seleznev with aggravated identify theft in violation of 18 U.S.C.§ 1028A. Section 1028A makes it a crime to transfer, possess or use, without lawful authority, "a means of identification" during and in related to certain specified offenses. 18 U.S.C.§ 1028A(a). Wire fraud, access device fraud and computer fraud are specified offenses under this statute. 18 U.S.C.§ 1028A(c)(4) and (5).

Each 1028A charge arises out of Seleznev's possession and transfer of a means of identification (a credit card number) of an individual victim. Count 39 is based on Seleznev's possession of the credit card number of D.K., who is a Washington resident that dined at Broadway Grill. Count 40 is based on Seleznev's possession of the credit card number of R.G., a Washington resident that dined at Red Pepper Pizza.

The government has proposed the Ninth Circuit pattern instruction for aggravated identity theft, which sets forth the following elements:

> First, the defendant knowingly transferred, possessed or used without legal authority a means of identification of another person;
>
> Second, the defendant knew that the means of identification belonged to a real person; and

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5200
SEATTLE, WASHINGTON 98101
(206) 553-7970

> Third, the defendant did so during and in relation to the crime of wire fraud or access device fraud.

Ninth Circuit Model Jury Instruction 8.83.

A credit card number is a "means of identification" within the meaning of Section 1028A. *See* 18 U.S.C. § 1028(d)(7)(D) (defining "means of identification" to include any "access device" as defined in section 1029(e)); 18 U.S.C.§ 1029(e)(1)(defining "access device" to include any "account number . . . that can be used . . . to obtain money, goods, services, or any other thing of value").

IV. EVIDENTIARY ISSUES

A. Particular Hearsay Issues

1. Defendant's Statements

The government will offer certain statements made by Seleznev. These statements are admissible as admissions of a party opponent. Fed. R. Evid. 801(d)(2)(A); *United States v. Burreson*, 643 F.2d 1344, 1349 (9th Cir. 1981). The government may offer all, some, or none of a defendant's statements at trial under Rule 801(d)(2). Defendant may not offer his own statements under this rule because they are not statements of the proponent's "party-opponent." *United States v. Ortega*, 203 F.3d 675, 682 (9th Cir. 2000) (party cannot offer his own statement as party admission).

The statements to be offered include numerous statements Seleznev made over the internet in the course of operating his business. These will include online chats and email communications that Seleznev made under the cover of his online nics. To admit these statements as party admissions (*i.e.*, to attribute them to Seleznev), the Court must make a preliminary finding pursuant to Federal Rule of Evidence 104 that proof has been introduced "sufficient to support a finding" that Seleznev (or a co-conspirator) was the person who made the statements. Fed. R. Evid. 104(b). The Ninth Circuit has held that the quantum of proof for this finding is the existence of "substantial evidence," which is a lower standard of proof than preponderance of the evidence. *United States v. Flores*, 679 F.2d 173, 178 (9th Cir. 1982). As discussed in the factual recitation above, there is more

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5200
SEATTLE, WASHINGTON 98101
(206) 553-7970

than "substantial evidence" that defendant was the user of the three relevant email accounts. In addition, the chats to be offered were discovered on Seleznev's laptop and iPhone. Accordingly, the Court should find pursuant to Rule 104 that these statements are admissible as party admissions.

Similarly, in some of the e-mail and chat communications, Seleznev manifested an adoption or belief of certain statements made by others. Under those circumstances, statements of others are admissible under Fed. R. Evid. 801(d)(2)(B), which provides that the statements of others may be admitted against the defendant as long as the defendant "manifested an adoption or belief in its truth." Fed. R. Evid. 801(d)(2)(B); *see also United States v. Williams*, 445 F.3d 724, 735 (4th Cir. 2006), *cert. denied*, 127 S.Ct. 314. "When a statement is offered as an adoptive admission, the primary inquiry is whether the statement was such that, under the circumstances, an innocent defendant would normally be induced to respond, and whether there are sufficient foundational facts from which the jury could infer that the defendant heard, understood, and acquiesced in the statement." *Id.*; *United States v. Kenny*, 645 F.2d 1323, 1340 (9th Cir.) (tape recorded statements of cooperating codefendant's "half of the conversation" admissible "to the extent 'adopted' by Kenny," and may "be treated as a group of adoptive admissions" under the rule), *cert. denied*, 452 U.S. 920 (1981).

Courts have recognized that e-mail statements are admissible under this theory where the defendant manifested an adopt or belief in the statement. *See, e.g.*, *Sea–Land Service, Inc. v. Lozen Intern., LLC*, 285 F.3d 808, 821 (9th Cir. 2002) (trial court abused its discretion in excluding e-mail of company employee which was incorporated and forwarded to by another employee with a message which "'manifested an adoption or belief in [the] truth' of the information contained in the original e-mail."); *United States v. Safavian*, 435 F.Supp.2d 36, 43 (D.D.C. 2006) (admitting e-mails under Rule 801(d)(2)(B) based on the "context and content of certain e-mails" which established the defendant "'manifested an adoption or belief' in the truth of the statements of other people as he forwarded their e-mails").

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5200
SEATTLE, WASHINGTON 98101
(206) 553-7970

2. Co-Conspirator Statements

Statements of Seleznev's co-conspirators (such as persons who assisted him in operating the website) are admissible under Federal Rule of Evidence 801(d)(2)(E). This rule provides that a "statement is not hearsay if . . . [it] is offered against a party and is . . . a statement by a co-conspirator of a party during the course and in furtherance of the conspiracy." For Rule 801(d)(2)(E) to apply, it is not necessary that the conspiracy be charged. *United States v. Samiento-Rozo*, 676 F.2d 146, 149 (5th Cir. 1982). Further, the evidentiary rules that apply to co-conspirators apply equally to co-schemers in a wire fraud scheme. *United States v. Stapleton*, 293 F.3d 1111, 1117 (9th Cir. 2002).

3. Records of Regularly-Conducted Activity and Rule 902 Certifications

The government will offer records of regularly-conducted activities of businesses, including records of Yahoo!, Western Union, PayPal, the Bureau of Prisons, and web service providers Black Lotus, Cloudflare and Nusphere. These records are admissible pursuant to Rule 803(6), which allows for admission of a record if it is made at or near the time of the events set forth therein, by a person with knowledge, and is kept in the course of regularly-conducted activity of a business or other organization, if it is the regular practice of the organization to make the record. Fed. R. Evid. 803(6). Incompleteness, ambiguities, and inaccuracies in records go to the weight to be given the evidence, not to its admissibility. *United States v. Catabran*, 836 F.2d 453, 458 (9th Cir. 1988).

Any person familiar with the record-keeping practices of the business is a sufficient foundational witness. Personal knowledge of the document is not required, and does not affect its admissibility. *United States v. Childs*, 5 F.3d 1328, 1334 (9th Cir. 1993) (the phrase "other qualified witness" is broadly interpreted to require "only that the witness understand the record-keeping system" at the particular organization). Furthermore, a record generated by a third party and received and relied upon in the ordinary course, such as an invoice, becomes a business record of the company relying

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5200
SEATTLE, WASHINGTON 98101
(206) 553-7970

upon it. *Childs*, 5 F.3d at 1333-34; *see United States v. Jawara*, 474 F.3d 565, 585 (9th Cir. 2007) ("[W]e would have no trouble concluding that a college in the United States was a proper custodian of its' students' SAT results, even though the SAT results were actually prepared by another entity"). In determining whether these foundational facts have been established, the court may consider hearsay and other evidence not admissible at trial. Fed. R. Evid. 104(a).

The government intends to authenticate these business records by offering Rule of Evidence 902(11) certifications rather than live testimony. Rule 902(11) provides that a party may authenticate a business record through a signed certification of records custodian if the proponent of the evidence gives the adverse party adequate notice of its intent to offer the record. The government has provided all 902(11)s to the defense. On July 18, 2016, the government requested that the defense notify the government of any objections to the 902 certifications. The government has not received any objections.

4. Defendant's Passport

The government intends to introduce Seleznev's international and internal passports, which were seized from him at the time of arrest. [3] The passports establish defendant's home address, passport numbers, names of his family members, and his travel history. Because the government does not have access to other records maintained by the Russian government, these documents are needed to prove these basic identifying facts about Seleznev. This evidence is a critical part of linking Seleznev to the criminal infrastructure. For example, defendant's passport number and the names of his family members appear on the HopOne server, and his address appears in the Rubenlsamvelich and Boookscafe Accounts.

A passport is admissible under various exceptions to the hearsay rule. First, the Ninth Circuit has held that a passport is admissible under the residual exception (Rule 807), which allows admission of a statement where the statement has circumstantial

[3] Russian citizens carry an internal passport as a means of identification.

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5200
SEATTLE, WASHINGTON 98101
(206) 553-7970

guarantees of trustworthiness, is evidence of a material fact, and is more probative on the point for which it is offered than any other piece of evidence. *United States v. Brown*, 770 F.2d 768, 771 (9th Cir, 1985) (district court properly admitted passports under Rule 803(24), which has since be been re-codified as Rule 807). Second, passports are admissible as public records under Rule 803(8). *United States v. Pluta*, 176 F.3d 43, 50 (2d Cir. 1999) (foreign passport properly admitted to show foreign citizenship); *United States v. Eltayib*, 88 F.3d 157, 169 (2d Cir. 1996) (foreign passports properly admitted to show passport holders' dates of entry into Venezuela). Third, where, as here, the passport belongs to the defendant and the defendant has presented it as identification to government officials (such as the Maldivian authorities and immigration officials of other countries), the passport becomes an adopted admission of the defendant. Fed. R. Evid. 801(d)(2)(B) (a statement is not hearsay if it is "one the party manifested that it adopted or believed to be true").

5. Statements Not Offered for Their Truth

Overview: Statements introduced for a non-hearsay purpose do not violate the hearsay rule. *See, e.g.*, *Anderson v. United States*, 417 U.S. 211, 219 (1974) ("Out of court statements constitute hearsay only when offered in evidence to prove the truth of the matter asserted."); *United States v. Jaramillo-Suarez*, 950 F.2d 1378, 1383 (9th Cir. 1991) (ledgers properly introduced not to show the amounts due, but the nature of the business conducted at a particular location).

The government will be offering many statements for purposes other than establishing their truth. For example, after Seleznev was arrested, one of his co-schemers posted a notice that the "boss" had "been in a car accident." The government will offer this statement not to establish that the boss of 2Pac had been in a car accident, but to show that the operators of the website were attempting to explain his absence. As another example, the government will offer testimony that, when Seleznev was presented with the indictment at the time of his arrest, Seleznev's immediate response was to protest that the United States did not have authority to extradite him from the Maldives.

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5200
SEATTLE, WASHINGTON 98101
(206) 553-7970

While this statement is also admissible as a party admission, is it not hearsay because it is offered to show Seleznev's reaction to the charges—not to establish the truth of whether authority existed to extradite him.

The government may also offer statements for their falsity. Such statements do not implicate the hearsay rule. *United States v. Fried*, 576 F.2d 787, 793 (9th Cir. 1978) (out of court statements not hearsay where offered for their falsity); *see also United States v. Adkins*, 741 F.2d 744, 746 (5th Cir. 1984) ("When the statements are introduced to prove the falsity of the matter asserted, they are not inadmissible as hearsay."). In addition to these obvious examples, discussed below are broad categories of non-hearsay evidence that may be offered at trial.

Machine-Generated Information: Some of the government's evidence will include machine-generated information. This includes the IP address, logs, date, time and screen names of defendant or co-conspirators. Information of this nature appears in places such as the header information in an email, screen names and time stamps in chat messages, or the metadata from files taken from a computer. The courts have consistently held that machine-generated information is not hearsay as no "person" is making a statement. *See, e.g., United States v. Hamilton*, 413 F.3d 1138, 1142-43 (10th Cir. 2005) (computer-generated "header" information including the screen name, subject of the posting, the date the images were posted, and the individual's IP address was not hearsay; no "person" was acting as a declarant); *United States v. Washington*, 498 F.3d 225, 231 (4th Cir. 2007) (machine-generated data used to determine whether a blood sample contained drugs or alcohol were not statements of the lab technicians and were not hearsay statements; they were made not by persons but machines analyzing the sample; no Confrontation Clause issues); *United States v. Khorozian*, 333 F.3d 498, 506 (3d Cir. 2002) (information automatically generated by fax machine is not hearsay since "nothing 'said' by a machine . . . is hearsay"), *cert. denied*, 540 U.S. 968 (2003).

Statements Offered to Supply Context: As noted above, the statements of the defendant on e-mails and chat communications are admissible as party admissions. The

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5200
SEATTLE, WASHINGTON 98101
(206) 553-7970

statements of others used in the e-mails and chat communications may be admitted as non-hearsay statements to supply context. *See, e.g., United States v. Burt*, 495 F.3d 733, 738-39 (7th Cir. 2007) (in a chat between the defendant and third party, the portion of the chat from the third party was admissible to help the jury understand the conversation), *cert. denied*, 128 S.Ct. 724 (2007); *United States v. Dupre*, 462 F.3d 131, 136-37 (2d Cir. 2006) (e-mails from third parties admissible when offered not for truth of the assertion, but to provide context for the defendant's response).

Here, the government anticipates admitting emails and chat messages, some of which may come in for their truth under the appropriate rule, such as co-conspirator statements and adoptive admissions, but at other times for reasons other than the truth of the matter asserted, for example as evidence of defendant's use of specific nicknames and passwords, such as "smaus,." The government will also offer evidence that receipts for parts of the criminal infrastructure (such as the HopOne server) were found in the Yahoo email accounts. Similar to ledgers found in a drug house offered to show the use of the premises for criminal purposes, these emails will be offered to show that the email accounts were used in furtherance of the fraud.

B. Admission of Electronic Evidence

Much of the government's evidence consists of electronic evidence, such as emails, online chats, computer files, and remnants of computer activity found within devices such as the HopOne server and defendant's laptop. Despite the digital nature of much of the government's evidence, the Rules of Evidence apply no differently than they do to physical evidence.

1. General - Authentication of Electronic Evidence

Authentication of evidence under Federal Rule of Evidence 901 is an "aspect of relevancy." Fed. R. Evid. 901(a), Advisory Committee Notes (1972 Proposed Rules). "To satisfy the requirement of authenticating or identifying an item of evidence, the proponent must produce evidence sufficient to support a finding that the item is what the proponent claims it is." Fed. R. Evid. 901(a). In doing so, "[t]he government need only

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5200
SEATTLE, WASHINGTON 98101
(206) 553-7970

make a prima facie showing of authenticity, as the rule requires only that the court admit evidence if sufficient proof has been introduced so that a reasonable juror could find in favor of authenticity or identification." *United States v. Black*, 767 F.2d 1334, 1342 (9th Cir. 1985) (internal quotes and citations omitted). This "rule is not a particularly high hurdle." *United States v. Ortiz*, 966 F.2d 707, 716 (1st Cir. 1992). Once a prima facie showing of authenticity has been made, any questions about accuracy or completeness are for the jury to consider in determining the weight to give to the evidence, and not to admissibility. *See United States v. Tank*, 200 F.3d 627, 630 (9th Cir. 2000) (quoting also *United States v. Catabran*, 836 F.2d 453, 458 (9th Cir. 1988) ("Any question as to the accuracy of the printouts…would have affected only the weight of the printouts, not their admissibility.").

Moreover, in making its determination, "the court is not bound by evidence rules, except those on privilege." Fed. R. Evid. 104(a). In proving authenticity, the government may utilize "circumstantial, as well as direct, evidence." *Black*, 767 F.2d at 1342 (citation omitted). Authenticity may be shown by "the appearance, contents, substance, internal patterns or other distinctive characteristics of the item, taken together with all the circumstances." Fed. R. Evid 901(b)(4); *see United States v. Jones*, 107 F.3d 1147, 1150, (6th Cir. 1997) ("[A] document…may be shown to have emanated from a particular person by virtue of its disclosing knowledge of facts known peculiarly to him…") (citing Fed. R. Evid. 901(b)(4), Advisory Committee Notes, Example (4)); *see also Alexander Dawson v. N.L.R.B.*, 586 F.2d 1300, 1302 (9th Cir. 1978) ("The content of a document, when considered with the circumstances surrounding its discovery, is an adequate basis for a ruling admitting it into evidence.") (citation omitted).

Furthermore, in regards to chain of custody, a sufficient chain of custody is established if a reasonable juror could conclude that the proffered evidence is in "substantially the same condition as when they were seized." *United States v. Harrington*, 923 F.2d 1371, 1374 (9th Cir. 1991)(quotations and citation omitted). In establishing chain of custody, "[t]here is no rule requiring the prosecution to produce as

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5200
SEATTLE, WASHINGTON 98101
(206) 553-7970

witnesses all persons who were in a position to come into contact with the article sought to be introduced in evidence." *Gallego v. United States*, 276 F.2d 914, 917 (9th Cir. 1960) (citation omitted). Moreover, gaps in a chain of custody "normally go to the weight of the evidence, rather than its admissibility." *United States v. Melendez-Diaz*, 557 U.S. 305, 311 n.1 (2009); *see also United States v. Matta-Ballesteros*, 71 F.3d 754, 769 (9th Cir. 1995) ("[A] defect in the chain of custody goes to the weight, not the admissibility, of the evidence introduced") (citations omitted); *Harrington*, 923 F.2d at 1374 ("The possibility of a break in the chain of custody goes only to the weight of the evidence.").

As it would with physical evidence, the government will authenticate its electronic evidence generally by agent testimony about where the evidence was seized, how it was copied from the electronic device, and what about the "appearance, contents, substance, internal patterns or other distinctive characteristics of the item, taken together with all the circumstances" makes it relevant to the defendant's case. Fed. R. Evid. 901(b)(4). Discussed below are several categories of evidence the government anticipates admitting into evidence, all of which were taken from the internet, digital devices, and seized computers and servers.

2. Screenshots of Undercover Operations

The government will offer screenshots of web pages (such as the Bulba and 2Pac website) taken by law enforcement officers during undercover operations and other online investigative activities. The screenshots will be authenticated by the law enforcement officers, who will testify that the screenshots are an accurate representation of the websites on the dates that they visited them. This is sufficient to support admission of the documents under Rule 901(b)(1), which allows for authentication by testimony of a witness with knowledge "that an item is what it is claimed to be." *United States v. Bansal*, 663 F.3d 634, 668 (3d Cir. 2011) (testimony from witness with knowledge of websites was sufficient to authenticate screenshots under Rule 901(b)(1)); *Thompson v. Bank of America N.A.*, 783 F.3d 1022, 1028 (5th Cir. 2015) ("in the case of . . . a website

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5200
SEATTLE, WASHINGTON 98101
(206) 553-7970

. . . testimony with direct knowledge of the source stating that it fully and accurately reproduces it, may be enough to authenticate"); *Osborn v. Butler*, 712 F. Supp. 2d 1134, 1146 (D. Idaho 2010) (printout of website properly authenticated by affidavit of witness who printed the page).

3. Online Chats

During trial, the government anticipates admitting chat logs verifying the Defendant's identity and his criminal activities. The evidentiary standard for chat logs is the same bar outlined in Fed. R. Evid. 901(a), that is that the chats are what they purport to be. *See Tank*, 200 F.3d at 630-631 (government made a *prima facie* showing of authenticity with testimony that the chats were accurate printouts, and establishing a connection with the chat logs and the defendant); *United States v. Masters*, 613 F. Appx. 618, 620-21 (9th Cir. 2015) (finding chat logs were properly authenticated because "a reasonable juror could conclude that the user" was the defendant based upon other evidence). Moreover, "[t]he issue of authenticity – the identity of the author of a particular item of evidence such as a document or phone call – is for the jury once a prima facie case of authorship is made out by the proponent of the evidence." *Carbo v. United States*, 314 F.2d 718 (9th Cir. 1986). "The issue for the trial judge in determining whether the required foundation for the introduction of evidence has been established is whether the proof is such that the jury, acting as reasonable men, could find it authorship as claimed by the proponent." *Id.*

To establish foundation for internet chats, witnesses will testify that the chats were found on defendant's laptop, and that they were printed from the computers accurately. In the case of chats found in places other than defendant's laptop, the government will provide extensive evidence linking the chats to Seleznev, thereby meeting the low threshold of a *prima facie* showing of authenticity. For example, the government will offer chats between defendant (using the alias nCuX111) and a third party in which nCuX111 identifies himself as Roman Seleznev and provides Roman Seleznev's address

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5200
SEATTLE, WASHINGTON 98101
(206) 553-7970

as a shipping address and the Booookscafe Account as his email address. This is sufficient *prima facie* evidence to support admission of these chats as statements of the defendant.

4. Emails

During trial, the government anticipates admitting evidence of emails from the following Booookscafe Account, Rubensamvelich Account, and Bulba Account (collectively the "Yahoo Accounts"). Based on the investigation, the Yahoo Accounts were all utilized by Seleznev to further his criminal schemes. In response to legal process, Yahoo! produced business records, which provided subscriber information for each of the Yahoo Accounts. The subscriber information identifies information such as the "Login Name," "Account Created" date, the "Full Name and "Address" provided by the user. Yahoo produced a Business Record Certification identifying the subscriber information as a duplicate of a record of regularly conducted activity that would be admissible under Rule 803(6). As such, the subscriber record information is admissible as a self-authenticating record under Fed. R. Evid. 902(11) and an exception to the rule against hearsay pursuant to Fed. R. Evid. 803(6).

In addition to the business records with subscriber information, Yahoo! produced emails which were contained within the Yahoo Accounts. From the produced emails, the government anticipates admitting approximately 40 separate emails found within the Yahoo Accounts. The government anticipates authenticating those records by means of a Rule 902(11) certification rather than through a Yahoo representative. In addition, the government will provide evidence that will be "sufficient to support a finding that the matter in question is what its proponent claims." Fed. R. Evid. 901(a). *See, e.g., United States v. Fluker*, 698 F.3d 988, 999-1000 (7th Cir. 2012) (finding that emails were properly authenticated through circumstantial evidence, including the content of the email itself); *United States v. Siddiqui*, 235 F.3d 1318, 1322-1323 (11th Cir. 2000) (finding that emails were properly authenticated through circumstantial evidence, including because the email address had been associated with the defendant). As

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5200
SEATTLE, WASHINGTON 98101
(206) 553-7970

discussed above, there is extensive evidence establishing that this email account was maintained by Seleznev.

5. Server Contents

In addition to emails from Yahoo!, the government anticipates admitting evidence stored on the HopOne server. A server is a computer that is often used for specific client services such as hosting a webpage or storing data. The HopOne server was used to receive data, such as stolen credit card data. Additionally, a user of the HopOne Server could log into it to conduct general computing activities, such as browsing the web.

Because the HopOne server contained data similar to how computers, hard drives and other digital storage devices hold data, the authentication process of its data is similar, that is by a witness with knowledge who can establish where the server was obtained, how it was examined, and what files were extracted from the server. *See, e.g., United States v. Salcido*, 506 F.3d 729, 733 (9th Cir. 2007) ("[T]he government properly authenticated the videos and images under Rule 901 by presenting detailed evidence as to the chain of custody, specifically how the images were retrieved from the defendant's computers."); *United States v. Whitaker*, 127 F.3d 595, 601 (7th Cir. 1997) (in conspiracy to distribute marijuana case, computer files were properly authenticated by an agent who testified that the records were seized from defendant's computer during a search warrant and that the agent participated in obtaining the computer printouts). The government will offer testimony from law enforcement agents authenticating the HopOne server.

6. Domain Registration Information

The government will offer evidence showing the publicly-available domain registration information for Seleznev's websites. As discussed above, a person seeking to establish a website must provide a registrar with certain registration information including his or her name and email address. These records, which are similar to telephone books for the internet, are shared publically across the internet in order to facilitate the proper routing of computer communications. Various companies, including

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5200
SEATTLE, WASHINGTON 98101
(206) 553-7970

a Seattle-based company named Domain Tools, maintain directories of this registration information. The information in these domain registration records is relied on by the public and those working in the computer networking industry. The government will offer reports produced by Domain Tools to establish, for example, that the Rubensamvelich Account was used to register the Track2 website.

The Domain Tools registration reports are admissible under Federal Rule of Evidence 803(17), which provides for the admissibility of "lists, directories, or other published compilations generally used and relied upon by the public or by persons in particular occupations." These domain registration reports are widely-relied upon, publicly-available documents of the sort repeatedly held admissible under Rule 807(17). *United States v. Woods*, 321 F.3d 361, 363-4 (3d Cir. 2003) (vehicle identification number recorded in national crime database admissible under Rule 807(17)); *United States v. Goudy*, 792 F.2d 664, 674 (7th Cir. 1986) (bank directory admissible to show routing number assigned to specific bank); *United States v. Anderson*, 532 F.2d 1218, 1222 (9th Cir. 1976) (publicly-available stock market reports admissible to show stock price recorded in those reports). They are also admissible as records of a regularly-conducted activity under Rule 803(6).

7. Nicknames

Much of the evidence at trial will display or connect Seleznev to nicknames he used throughout his criminal activity. "As many courts have recognized, a prosecutor may introduce evidence of a defendant's alias or nickname if this evidence aids in the identification of the defendant or in some other way directly relates to the proof of the acts charged in the indictment." *United States v. Williams*, 739 F.2d 297 (7th Cir. 1984). *See also United States v. Kalish*, 690 F.2d 1144, 1155 (5th Cir.1982), cert. denied, 459 U.S. 1108, 103 S.Ct. 735, 74 L.Ed.2d 958 (1983) (defendant's alias admissible where it was used to conceal identity from arresting officer).

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5200
SEATTLE, WASHINGTON 98101
(206) 553-7970

C. Defendant's Interview With Law Enforcement

On December 19, 2014, Seleznev participated in a voluntary interview with law enforcement. During this interview, Seleznev admitted substantially all conduct charged in the Second Superseding Indictment, including the fact that he was the true identity behind nCuX, Track2, Bulba and 2Pac.

As the Court is aware, Seleznev made these statements pursuant to an agreement providing that his statements could be used against him at trial only if (a) he testified contrary to his interview statements, or (b) his attorneys took positions at trial contrary to those statements. On April 29, 2016, the Court granted in part defendant's motion to limit this agreement. The Court found that, when he signed the agreement, Seleznev may not have understood the portion of the agreement allowing use of his admissions based on the conduct of his attorneys.

However, the Court found that ethical rules nonetheless preclude counsel from taking positions that they know are contrary to their client's admissions. Accordingly, the Court held that defense counsel "will not be permitted to elicit substantive, non-impeachment testimony, either on cross-examination of witnesses called by the government or from witnesses called to testify on behalf of the defendant or to present arguments to the jury at any stage of the proceedings that directly contradict specific factual statements made by the defendant" during the interview. Dkt 328 at 7. The government has filed a motion *in limine* setting out the scope of Seleznev's admissions and proposing a procedure for enforcing this Order at trial. Dkt. 360. Defendant has also filed a motion addressing this issue. Dkt. 364.

D. Expert Testimony

1. Admissibility of Expert Testimony

Federal Rule of Evidence 702 governs the admission of expert testimony. It is based on the recognition that "an intelligent evaluation of the facts is often difficult or

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5200
SEATTLE, WASHINGTON 98101
(206) 553-7970

impossible without the application of specialized knowledge." Rule 702 Adv. Comm. Note. Rule 702 provides:

> If scientific, technical, or other specialized knowledge will assist the trier of fact to understand the evidence or to determine a fact in issue, a witness qualified as an expert by knowledge, skill, experience, training, or education, may testify thereto in the form of an opinion or otherwise, if (1) the testimony is based upon sufficient facts or data, (2) the testimony is the product of reliable principles and methods, and (3) the witness has applied the principles and methods reliably to the facts of the case.

Fed. R. Evid. 702.

In the *Daubert* decision, the Supreme Court adopted a flexible test for determining whether to admit scientific expert testimony under Rule 702. *Daubert v. Merrell Dow Pharm., Inc.*, 509 U.S. 579, 588 (1993). The Supreme Court later extended *Daubert* to apply to "technical or other specialized knowledge." *Kumho Tire Co. v. Carmichael*, 526 U.S. 137, 147 (1999). However, *Kumho Tire* rejected the proposition that the *Daubert* factors should be rigidly applied, stating instead that those factors "may or may not be pertinent in assessing reliability, depending on the nature of the issue, the expert's particular expertise, and the subject of his testimony." *Kumho*, 526 U.S. at 138.

While *Daubert* directs trial courts to serve as "gatekeepers" by excluding testimony that is genuinely unreliable, the gatekeeper role "is not intended to serve as a replacement for the adversary system." Fed. R. Evid. 702 Adv. Comm. Notes (quoting *United States v. 14.38 Acres of Land*, 167 F.3d 155 (5th Cir. 1996)). Indeed, *Daubert* itself made clear that "vigorous cross examination, presentation of contrary evidence, and careful instruction on the burden of proof are the traditional and appropriate means of attacking shaky but admissible evidence." *Daubert*, 509 U.S. at 595. Further, the Ninth Circuit has stated that Rule 702 should be "construed liberally," as a rule of inclusion and not of exclusion. *United States v. Hankey*, 203 F.3d 1160, 1168-69 (9th Cir. 2000) (expert testimony on gang activity properly admitted as specialized knowledge where expert had extensive personal observations of gangs; "Rule 702 works well for this type of data gathered from years of experience and special knowledge").

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5200
SEATTLE, WASHINGTON 98101
(206) 553-7970

An expert witness is not limited to providing opinion testimony. To the contrary, Rule 702 expressly provides that an expert "may testify in the form of an opinion *or otherwise*." (Emphasis added); *see* Rule 7 Adv. Comm. Notes (noting that "the assumption that experts testify only in the form of opinions" is "logically unfounded," and that "an expert on the stand may give a dissertation or exposition of scientific or other principles relevant to the case" without testifying in the form of an opinion). Much of the government's expert testimony will consist of experts explaining technical issues, but not necessarily in the form of an opinion.

2. The Government's Expert Testimony

The government disclosed its expert testimony to the defense on January 12, 2016, with supplemental notices on March 2, 2016 and April 27, 2016. These disclosures are attached to this Trial Brief as Exhibit A, and describe in detail the scope of expected testimony. The government provides the following brief summaries of expert testimony that may be adduced at trial, while reserving the right to present all testimony described in the notices.

Detective David Dunn: Since August 2014, Detective Dunn has been a strategic advisor to the Seattle Police Department ("SPD") and a part-time member of the USSS Electronic Crimes Task Force ("ECTF"). Before that, Detective Dunn spent 14 years with SPD and previously served as a full-time member of the USSS ECTF for seven years.

In February 2013, Detective Dunn left full-time government service to become the Director of Global Incident Response for Fidelity Information Services, the world's largest provider of financial service technology. Detective Dunn is currently employed as the Deputy Chief Information Security Officer for Kroll and Associates, a computer security incident response and remediation company where he has been employed since February 2016. In the course of his career, Detective Dunn has developed expertise and specialized knowledge about computer systems and networks, network intrusions (specifically point of sale intrusions), computer forensics, credit card payment processing

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5200
SEATTLE, WASHINGTON 98101
(206) 553-7970

systems, the underground carding industry, and the fraudulent use of credit card data. Detective Dunn was the original investigating officer on this case.

Detective Dunn will provide the jury with an overview of technical issues relating to the internet, computer systems, network intrusions and payment systems. For example, Detective Dunn will explain principles relevant to the operation of the internet such as the use of internet protocol ("IP") addresses and the methods by which websites are registered and hosted. He will explain the role of servers and other types of computer infrastructure, and will explain the operation of web-based email such as the Yahoo! email accounts at issue here. Detective Dunn will explain the basic operation of point of sale ("POS") systems and also the way in which credit cards are encoded and processed.

Detective Dunn will also testify about the *modus operandi* of carders and hackers. The Ninth Circuit has held that testimony of this nature is admissible under Rule 702. *United States v. Anchrum*, 590 F.3d 795, 804 (9th Cir. 2009) (law enforcement officer properly testified about *modus operandi* of gangs he had investigated); *United States v. Vallejo*, 237 F.3d 1008, 1016 (9th Cir. 2001) (expert testimony on *modus operandi* of drug dealers admissible); *United States v. Plunk*, 153 F.3d 1011, 1017 (9th Cir. 1998), *overruled on other grounds, United States v. Hankey*, 203 F.3d 1160, 1169 n.7 (9th Cir. 2000) (approving expert testimony on jargon and coded language of criminals). Specifically, Detective Dunn will testify about the methods that hackers use to intrude into POS systems and other computers. As part of this testimony, Detective Dunn will discuss malware generally and the operation of the specific malware that Seleznev utilized in this case. Detective Dunn also will discuss the international carding community and explain the role of carding forums and automated vending sites. Detective Dunn will also testify about the meaning of slang and jargon used in the carding community. Detective Dunn examined many of the victim computers in this case and will provide specialized testimony relevant to those examinations.

As discussed above, Detective Dunn was the case agent on this matter and will provide both fact testimony and expert testimony. Because of the inherently complex

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5200
SEATTLE, WASHINGTON 98101
(206) 553-7970

nature of computer hacking and network intrusion investigations, cybercrime investigators such as Detective Dunn employ specialized knowledge and expertise in nearly every step of their investigations. Accordingly, explaining their investigative steps (the type of testimony considered purely fact testimony for other types of law enforcement officers) necessarily involves explaining specialized matters. The Ninth Circuit has held that, where a witness will give dual fact and expert testimony, "a cautionary instruction on the dual role of such a witness must be given." Comment to Ninth Circuit Model Jury Instruction 4.14A (*citing United States v. Vera*, 770 F.3d 1232, 1246 (9th Cir. 2014). The government is proposing that the Court provide Ninth Circuit Model Instruction 4.14A to address this issue.

Special Agents David Mills and Michael Fischlin: Special Agent David Mills is a Seattle-based USSS agent and forensic examiner. Special Agent Michael Fischlin is a former Seattle-based USSS agent and forensic examiner. Special Agent Fischlin served as case agent on this matter between July 2014 and May 2016. Special Agent Fischlin is presently an agent with the United States Postal Inspection Service.

Special Agents Mills and Fischlin both participated in the forensic analysis of the laptop seized from Seleznev at the time of his arrest. They will provide specialized testimony about forensic analysis and the contents of the laptop. In addition, Special Agent Fischlin examined the computer systems of one of the victims in this case (Red Pepper Pizza) and will testify about specialized matters relating to that examination.

Detective Chris Hansen: Detective Hansen is a member of the Seattle Police Department and the USSS Electronic Crimes Task Force. Detective Hansen is an experienced forensic examiner and is also experienced in investigating identify theft and credit card fraud. Detective Hansen conducted the forensic examination of Seleznev's iPhone and is expected to testify about specialized matters relating to this examination.

Special Agent John Szydlik: Special Agent Szydlik is a Washington, DC-based agent with the USSS Cyber Intelligence Section. Special Agent Szydlik has extensive experience with the Liberty Reserve e-payment system that Seleznev used to collect

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5200
SEATTLE, WASHINGTON 98101
(206) 553-7970

payment for the stolen credit card data he sold under the nCuX, Track2, and Bulba nics. Agent Szydlik is familiar with the Liberty Reserve records, which were seized by law enforcement in May 2013 and will testify about the portions of the records that show Seleznev receiving payment for stolen credit card data under the nCuX, Track2, and Bulba nics.[4] Agent Szydlik also conducted an investigation into the 2pac website and made undercover purchases from that website before Seleznev's arrest. Special Agent Szydlik may testify about specialized matters in describing those activities and the operation of the website.

Matthew Geiger: Mr. Geiger is a specialist in malware analysis and presently works as a Senior Security Researcher for Dell Secureworks. Before joining Secureworks, Mr. Geiger worked for the United States Computer Emergency Readiness Team (US-CERT), a component of the Department of Homeland Security whose mission includes responding to computer security incidents and analyzing data about emerging cyber threats.

Mr. Geiger analyzed three different versions of the malware that Seleznev installed on victim machines. Mr. Geiger will testify about the functionality of the malware, the way in which it was packaged and installed, and how it sent stolen credit card data over the internet to remote servers.

Tim Chen: Mr. Chen is a corporate officer of Domain Tools, a Seattle-based company that maintains registration information for websites including those operated by

---

[4] As a person familiar with the Liberty Reserve records, Special Agent Szydlik is qualified to authenticate and testify about the records under Rule 803. *See United States v. Ray*, 930 F.2d 1368, 1370 (9th Cir. 1990) (investigator properly permitted to authenticate corporate records because she "was familiar with" the record in question, had personally examined the records, and demonstrated a thorough understanding of the company's preparation and maintenance of records); *see also States v. Hathaway*, 798 F.2d 902 (6th Cir. 1986) ("[T]here is no reason why a proper foundation for application of Rule 803(6) cannot be laid, in part or in whole, by the testimony of a government agent or other person outside the organization whose records are sought to be admitted. . . . [A]ll that is required is that the witness be familiar with the record keeping system."); *United States v. Franco*, 874 F.2d 1136, 1139-40 (7th Cir. 1989) (holding that an agent's "thorough description of the bookkeeping process" qualified him to authenticate business records under Rule 803(b) despite not being custodian).

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5200
SEATTLE, WASHINGTON 98101
(206) 553-7970

the defendant. Mr. Chen may discuss specialized matters pertaining to domain registration, hosting, and related issues.

Grayson Lenik: Mr. Lenik is a private digital forensic investigator who was hired by many of Seleznev's victims to investigate and remediate Seleznev's intrusions into their computer systems. Mr. Lenik may testify about his analyses of these systems, which may involve testimony about specialized matters.

E. Charts and Summaries

The government will offer various charts and summaries, many of which are discussed in response to defendant's motions *in limine*. These summaries are admissible under Federal Rule of Evidence 1006, which provides in pertinent part:

> The contents of voluminous writings, recordings, or photographs which cannot conveniently be examined in court may be presented in the form of a chart, summary, or calculation.

Fed. R. Evid. 1006. "The purpose of the rule is to allow the use of summaries when the documents are unmanageable or when the summaries would be useful to the judge and jury." *United States v. Rizk*, 660 F.3d 125, 1130 (9th Cir. 2011).

Summary evidence is admissible if the underlying materials upon which the summary is based (1) are admissible in evidence; and (2) were made available to the opposing party for inspection. Fed. R. Evid. 1006; *Rizk*, 660 F.3d at 1130. The availability requirement ensures that the opposing party has an opportunity to verify the reliability and accuracy of the summary prior to trial. *Rizk*, 660 F.3d at 1130. The underlying materials must be admissible, but need not themselves be admitted into evidence. *Id.* at 1130.

F. Demonstrative Exhibits

The government also intends to use various demonstrative charts during its opening statement, examinations of witnesses, and in closing argument. Such charts include, for example, charts setting out the computer infrastructure Seleznev used in his intrusions and data trafficking. Such charts are permissible to assist the jury in understanding the

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5200
SEATTLE, WASHINGTON 98101
(206) 553-7970

evidence, even if they are not themselves admissible. *United States v. Stephens*, 779 F.2d 232, 238 (5th Cir. 1985) (simple flow charts tracing the defendant's use of loan proceeds).

The Ninth Circuit has determined that courts should take three precautionary measures when demonstrative charts are used: (1) review the charts to determine if information contained in them is supported by proof; (2) allow charts to be used as testimonial aids for witnesses and visual aids for counsel in argument, but not admit the charts in evidence or allow their use during jury deliberation; and (3) instruct the jury that the charts are an explanation of other evidence and not proof per se. *United States v. Abbas*, 504 F.2d 123, 125 (9th Cir. 1974). The jury should be told the charts are presented as a matter of convenience and if found to be inaccurate they should be disregarded entirely. The government is proposing Ninth Circuit Model Instruction 4.15, which contains this cautionary language.

G. Redaction of Credit Card Numbers and Certain Other Information

Local Civil Rule 5.2 provides for the redaction from exhibits of certain information, including passport numbers, dates of birth and "financial accounting numbers." In certain circumstances in this case, however, redaction of this information from trial exhibits is impractical and not necessary.

In many situations, the information that would be redacted *is the evidence* that must be presented to the jury. For example, Seleznev's passport number and date of birth appear in various places in the infrastructure used to commit the crimes. To link defendant to the crime, the government needs to display defendant's passport number and date of birth to the jury to show that the information saved on the computers in the criminal infrastructure actually matches the information found on defendant's person at the time of arrest. Similarly, in the case of credit card numbers, the existence of stolen credit card numbers on defendant's computer is evidence tying defendant to the fraud. The government therefore needs to display the credit card numbers to the jury.

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5200
SEATTLE, WASHINGTON 98101
(206) 553-7970

The risk that this information will be misused based on its display at trial is remote or non-existent. The government will not publicly file any documents containing personal identifying information. To the extent that the exhibits are filed in the court records, they will be filed under seal. Further, it is extremely unlikely that any of the credit card numbers remain active. All of the numbers were compromised between approximately two and eight years ago, and the USSS has informed the credit card issuers that these numbers have been compromised. Given these factors, the government does not intend to redact the credit card numbers from its exhibits.

H. Request to Accommodate Travel Schedule of Detective Dunn

As the government previously informed the court staff at the time of scheduling the trial, Detective Dunn, who is now a civilian witness, has a longstanding international family trip planned to begin on August 20. Detective Dunn will be called as one of the government's first witnesses, and the government expects that his direct testimony will be complete by mid-day on Thursday, August 18. In the event that the defense does not conclude its cross examination of Detective Dunn on August 19, the government requests that cross examination of Detective Dunn be continued until Tuesday August 30, when he returns to the United States.

I. Disposition of Forfeiture Allegations

1. Overview

Criminal forfeiture is *not* an element of the charged offenses. Rather, it is a form of punishment that may be imposed as part of the criminal sentence. *Libretti v. United States*, 516 U.S. 29, 39-40 (1995). The government must establish the forfeitability of property by a preponderance of the evidence. *United States v. Martin*, 662 F.3d 301, 307 (4th Cir.2011); see also *United States v. Rutgard*, 116 F.3d 1270, 1293 (9th Cir. 1997); *United States v. Hernandez-Escarsega*, 886 F.2d 1560, 1576-77 (9th Cir. 1989).

The procedures for determining the forfeitability of assets in criminal cases are set forth in Federal Rule of Criminal Procedure 32.2. The forfeiture phase of the trial occurs following a verdict of guilty on the counts that support the forfeiture. Fed. R. Crim. P.

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5200
SEATTLE, WASHINGTON 98101
(206) 553-7970

32.2(b)(1)(A). The question before the fact finder is "whether the government [has established the] requisite nexus between the property and the offense." Rule 32.2(b)(1)(A). The nexus that the government must show depends on the statutory basis for forfeiture—"constituting, or derived from, proceeds…obtained directly or indirectly, as the result of such violation." 18 U.S.C. § 982(a)(2).

A fact finder may base its forfeiture determination on evidence already in the record, as well as any additional evidence or information submitted by the parties. Fed. R. Crim. P. 32.2(b)(1)(B). Because forfeiture is part of sentencing, the Rules of Evidence do not apply. *United States v. Capoccia*, 503 F.3d 103, 109 (2d Cir.2007). Accordingly, hearsay may be considered and relied upon so long as it has sufficient indicia of reliability. *Id.*

2. The Court, Not a Jury, Should Determine Relevant Forfeiture Issues

Rule 32.2(b)(1) draws a distinction between two kinds of forfeitures – forfeiture of "specific property" and "personal money judgments." Where the government seeks a money judgment for the amount of the proceeds of the defendant's crime, there is no nexus determination to be made by the jury and the defendant is not entitled to a jury determination on the amount of the money judgment. *United States v. Tedder,* 403 F.3d 836, 841 (7th Cir. 2005) ("Rule 32.2 does not entitle the accused to a jury's decision on the amount of the forfeiture"); *United States v. Phillips,* 704 F.3d. 754, 771 (9th Cir. 2012) ("Given that the only issue here was a monetary forfeiture, no jury determination was necessary.").[5]

In the instant case, the government is seeking a personal money judgment and not the forfeiture of specific property. The Superseding Indictment provides Seleznev with notice that, pursuant to 18 U.S.C. §§ 982(a)(2)(A), 982(a)(1)(B), and 1030(i)(B), upon his conviction of Wire Fraud, in violation of 18 U.S.C. § 1343, Intentional Damage of a

[5] Rule 32.2(b)(1)(A) establishes that the government may seek a personal money judgment against the defendants. *See also United States v. Casey,* 444 F.3d 1071, 1077 (9th Cir. 2006) (a money judgment is warranted in a criminal case against a convicted defendant even if the defendant is insolvent).

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5200
SEATTLE, WASHINGTON 98101
(206) 553-7970

Protected Computer, in violation on 18 U.S.C. §§ 1030(a)(5(A) and 1030(c)(4)(B)(i), Obtaining Information from a Protected Computer, in violation of 18 U.S.C. §§ 1029(a)(2) and (3), and/or Possession of Fifteen or More Unauthorized Access Devices, in violation of 18 U.S.C. §§ 1029(a)(3) and (c)(1)(A)(i), the government will seek a money judgment of a sum of money representing the proceeds of those offense charged. As a money judgment does not require a jury's nexus determination, the government does not request that the jury determine the amount of the money judgment.

J. Translations

Approximately 40 of the government's trial exhibits are partially or completely written in the Russian language. The government has prepared translations of each of these exhibits. The translations have been marked as trial exhibits (for example, the translation of Exhibit 5.4 is labeled 5.4a, the translation of Exhibit 5.5 is labeled 5.5a, and so on). The government has provided all of the translations to the defense. The defense has not objected to the accuracy of any of the translations.

As one of its first witnesses, the government intends to call translator Andrei Medvedev. Mr. Medvedev has been a Washington State court-certified interpreter since 2010 and has been an active court interpreter since that time, testifying at various levels of state and federal courts. Mr. Medvedev will testify that he has either created or reviewed all of the translations, and that all of them are accurate translations of the Russian original. Based on this testimony, the government will request that the translations be admitted conditionally upon the admission of the Russian originals.

A translation of an otherwise admissible document is admissible based on a qualified interpreter's testimony that the interpretation is accurate. *United States v. Khan*, 794 F.3d 1288, 1294 (11th Cir 2015) (trial court properly admitted translations that contained translator's bracketed notes explaining the meaning of certain passages). Challenges to the accuracy of the translation do not go to their admissibility. *Id.* Rather, the defendant may challenge the interpretations on cross examination, or by offering his own translation, "thereby allowing the jury to make the final decision as to which

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5200
SEATTLE, WASHINGTON 98101
(206) 553-7970

translation it [finds] most credible." *Id.* The government has proposed a limiting instruction based on the one approved by the *Shah* court, which instructs the jury that it should assess for itself whether the translation is accurate based on factors such as the qualifications of the translator.

K. Exclusion of Witnesses

Pursuant to Rule 615 of the Federal Rules of Evidence, the government respectfully requests that witnesses be excluded from the courtroom, with the exception of the case agent, Special Agent David Mills. *United States v. Thomas*, 835 F.2d 219, 222-23 (9th Cir. 1987) (case agent permitted to remain in court through trial as a representative of the government); *see also United States v. Machor*, 879 F.2d 945, 953-54 (1st Cir. 1989) (same).

//

//

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5200
SEATTLE, WASHINGTON 98101
(206) 553-7970

V. CONCLUSION

This Trial Brief is intended to familiarize the Court with the government's case and evidentiary issues related to the trial presentation. The government will supplement this brief as necessary if additional issues arise.

DATED this 25th day of July, 2016.

Respectfully submitted,

ANNETTE L. HAYES
United States Attorney

s/ Norman M. Barbosa
NORMAN M. BARBOSA
Assistant United States Attorney

s/ Seth Wilkinson
SETH WILKINSON
Assistant United States Attorney

Western District of Washington
700 Stewart Street, Suite 5220
Seattle, Washington 98101-1271
Email: Norman.Barbosa@usdoj.gov
Email: Seth.Wilkinson@usdoj.gov

LESLIE R. CALDWELL
Assistant Attorney General

s/ Harold Chun
HAROLD CHUN
Trial Attorney
Computer Crime and Intellectual Property Section

CERTIFICATE OF SERVICE

I hereby certify that on July 25, 2016, I electronically filed the foregoing with the Clerk of Court using the CM/ECF system which will send notification of such filing to the attorneys of record for the defendant.

s/Janet K. Vos

JANET K. VOS
Paralegal Specialist
United States Attorney's Office
700 Stewart Street, Suite 5220
Seattle, Washington 98101-1271
Phone: (206) 553-7970
Fax: (206) 553-0755
E-mail: Janet.Vos@usdoj.gov